

## REMARKS

Favorable reconsideration and allowance of the claims of the present application are respectfully submitted.

In the present office action, Claims 5, 9 and 16 were rejected under 35 U.S.C. 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. The Examiner particularly objected to the recited language directed to “with a probability close to certainty” in Claims 5, 9 and 16. Applicants note that similar language is present in currently Claims 1, 7, 10, 12, 14 and 18.

As a preliminary matter, each of Claims 5-6, 8-13 and 15-17 are being canceled herein without prejudice. That is, in order to expedite prosecution of the present invention, these claims are being canceled with full rights reserved in filing one or more continuation applications directed to the canceled claims. Thus, the rejections of Claims 5, 6 and 9 under 35 U.S.C. 112, second paragraph, is respectfully obviated.

Claims 1, 7, 10, 12 and 14 further stand rejected under 35 U.S.C. 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. Particularly, the Examiner indicates that these claims are “unclear” in that there is no description as to 1) how the signature is generated; 2) to where the public key is provided, and 3) how the verification is performed.

Claims 9, 10 and 12 were further rejected under 35 U.S.C. 101, as allegedly being directed to non-statutory subject matter. In response, applicants have canceled Claims 9-10 and 12 thereby obviating the rejection under 35 U.S.C. 101.

The Examiner did indicate that Claims 1, 7, 10, 12 14 and 18 presented patentable subject matter if amended to overcome the rejections under both 35 U.S.C. 112, second paragraph, and 35 U.S.C. 101. Claims 2-4 and 8 are objected to as being dependent upon a rejected base claim but would be allowable if rewritten in independent form to include all of the limitations of the base claim and any intervening claims.

In response, Applicants amend Claims 1, 7, 14 and 18 to further provide recitations addressing the alleged instances of indefiniteness as indicated by the Examiner.

With respect to the alleged first instance of indefiniteness articulated in the office action: Claims 1, 7, 14 and 18 are being amended to set forth that

the deriving of the signature value includes: computing an  $e$ -th root of a value derived from the message and the secret key using a cryptographic hash function, the  $e$  being an exponent value from exponent interval  $I$ . Respectfully, no new matter is being entered as full support is found in Fig. 3, processing in boxes 34 and 36 and the discussion at the first full paragraph of page 10 of the originally filed specification.

With respect to the alleged second instance of indefiniteness articulated in the office action: Claims 1, 7, 14 and 18 are being amended to set forth that the recited public key value ( $n$ ,  $h$ ,  $x$ ,  $e'$ ) of the public key which is shown as element 42 in Fig. 4, is provided to the second computing node where the verification of the signature value takes place. Respectfully, no new matter is being entered.

With respect to the alleged third instance of indefiniteness articulated in the office action: Claims 1, 7, 14 and 18 are being amended to set forth the verification procedure at the second computing node as shown in Fig. 4 where verification of said signature value at said second

computer node, includes raising the computed signature root value that forms part of the signature value to the power of the exponent value  $e$ , and, from said provided public key value, confirming that said exponent value  $e$  is contained in an exponent interval  $I$  having said plurality of exponent elements.

Respectfully, no new matter is being entered as these two verification actions preformed at a second computer node are shown in element 44 of Fig. 4 and described at page 10, lines 10-24. It is noted in the amendment to Claims 1, 7, 14 and 18 care has been taken to remove the objected to recitation “with a probability close to certainty” as articulated in the rejection of Claims 5, 9 and 16 (now canceled).

Further amendments are being provided to correct antecedent problems with recitations “said interval” and “said secret key” in Claims 1 and 14.

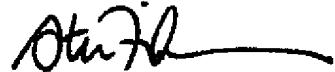
Thus, in view of the foregoing amendments and remarks, the Examiner is respectfully requested to withdraw the rejections of independent Claims 1, 7, 14 and 18 under 35 U.S.C. 112, second paragraph.

While applicants note that Claims 5, 9 and 16 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Brennan et al. (U.S. Patent No. 5,675,649) in view of Lambert et al. (U.S. Patent No. 7,127,063) and, that Claim 6 is rejected as allegedly unpatentable over Brennan et al. in view of Lambert et al. in further view of Matyas et al. (U.S. Patent No. 5,265,164) applicants have canceled Claims 5, 9 and 16 without prejudice, thereby obviating the rejections under 35 U.S.C. § 103(a).

In view of the foregoing, this application is now believed to be in condition for allowance, and a Notice of Allowance is respectfully requested. If the Examiner believes a

telephone conference might expedite prosecution of this case, it is respectfully requested that he call applicant's attorney at (516) 742-4343.

Respectfully Submitted,



Steven Fischman  
Registration No. 34,594

Scully, Scott, Murphy & Presser, P.C.  
400 Garden City Plaza, Suite 300  
Garden City, New York 11530  
(516) 742-4343

SF:gc